UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF TEXAS
BEAUMONT DIVISION

Angela Steinhardt, *Plaintiff*, v. albertAI.click, Lena Doe, and John Does 1 – 20, *Defendants*.	Case No. 1:25-cv-00303 **Plaintiff's Motion for *Ex Parte* Temporary Restraining Order & Order Authorizing Expedited Discovery**

Plaintiff Angela Steinhardt hereby requests that the Court enter (i) a temporary restraining order freezing the Defendants' assets and (ii) an order authorizing her to engage in expedited discovery. In support, Dr. Steinhardt respectfully shows the Court as follows.

I. Preliminary Statement

Dr. Steinhardt filed this action to recover assets she lost to a cryptocurrency-related fraud and conversion scheme operated by a sophisticated criminal syndicate. The Defendants stole assets worth approximately $372,000 from Dr. Steinhardt—a devastating loss. Sadly, Dr. Steinhardt is not alone. She is but one victim of the ongoing crypto-fraud epidemic, to which hardworking Americans are losing billions every year.

As is typical in crypto-fraud cases, Dr. Steinhardt does not know the Defendants' true identities or their precise whereabouts. But, with the assistance of a professional blockchain investigator, she has traced her stolen assets to accounts and addresses controlled by the Defendants. This tracing is fundamental to the relief Dr. Steinhardt seeks in this Motion. It is her foothold in the arduous climb toward recovery.

Dr. Steinhardt's present aims are to preserve the status quo and serve the Defendants with process. Accordingly, she now seeks (i) an *ex parte* temporary restraining order freezing the Defendants' assets and (ii) authorization to issue subpoenas to various third parties seeking information about the Defendants and their activities.

II. Supporting Materials

Dr. Steinhardt submits the following materials in support of this Motion.

Exhibit 1: Cole Declaration. Evan Cole is Plaintiff's investigator in this case. Mr. Cole's declaration attests to information about the pig-butchering epidemic, cryptocurrency technology, and blockchain-tracing methodology. It also provides the blockchain-tracing report showing the locations to which the assets misappropriated from Dr. Steinhardt were ultimately transferred.

Exhibit 2: Hoda Declaration. Marshal Hoda is counsel to Dr. Steinhardt in this matter. Counsel's declaration attests to the reasons why the Court should not require notice before issuance of an *ex parte* temporary restraining order.

III. Factual Allegations

This section first provides necessary background about the crypto-fraud epidemic. It then explains salient aspects of blockchain technology and tracing methodology. Finally, it summarizes the facts of this case and details the tracing of the assets the Defendants stole from Dr. Steinhardt.

A. The Pig-Butchering Epidemic

This case arises from what is known as a "pig-butchering scam." In such scams, the perpetrators convince the victim to either trade assets or offer employment on a fake-but-realistic-looking online platform that the perpetrators control.[1] No trading actually takes place and any employment opportunity is a ruse.[2] The perpetrators simply steal the victim's money, then disappear into cyberspace.[3]

Pig-butchering syndicates' mechanics are well known. The largest pig-butchering organizations are based in Southeast Asia, where this type of scam originated.[4] They are managed at the highest level by professional criminals, who use forced labor to fill their operations' rank-and-file.[5] These

---

[1] *See* Ex. 1, Declaration of Evan Cole (henceforth "Cole Declaration"), ¶¶ 3 – 4 (describing pig-butchering epidemic and providing sources).

[2] *Id.*

[3] *Id.*

[4] *Id.*

[5] *Id.*

'agents' are trained in social-engineering and psychological-manipulation techniques, which they use to deceive and steal from the syndicates' victims.[6]

B. Dr. Steinhardt's Allegations

This Defendants' scheme bears the unmistakable characteristics of a pig-butchering scam.[7] Lena Doe contacted Dr. Steinhardt through WhatsApp and gained her trust by patiently building a professional relationship.[8] She assisted her in making an account on the albertAI.click platform, and "trained" her for a new position.[9] Dr. Steinhardt began working and was even able to withdraw funds, making the platform appear legitimate.[10]

But when Dr. Steinhardt attempted to withdraw her $800,000 "Lucky 7 Anniversary Celebration" commission, she was told she needed to pay various fees in the amount of $372,000.[11] Dr. Steinhardt paid these fees but was still unable to retrieve any of her funds. Dr. Steinhardt then realized she had been the victim of a scam.[12]

---

[6] *Id.*

[7] *Id.*

[8] Complaint, ¶ 13 – 18.

[9] *Id.*

[10] *Id.*

[11] *Id.*

[12] *Id.*

The cryptocurrencies Dr. Steinhardt transferred to the Defendants were never used for any legitimate purpose.[13] The Defendants simply stole Dr. Steinhardt's assets. They are now running away with those assets by transferring them from address to address on the blockchain.[14]

C. Blockchain Background

This section provides background necessary to appreciate Dr. Steinhardt's blockchain-tracing evidence, and, in turn, why she has satisfied the legal standards applicable to this Motion. It first sets out cryptocurrency fundamentals, then details the practice of "blockchain tracing," and finally explains crucial points about the recoverability of crypto assets.

1. Cryptocurrency Fundamentals

A "blockchain" is a distributed and immutable ledger that facilitates the process of recording transactions and tracking assets.[15] A cryptocurrency, in turn, is a digital asset that is created, distributed, and transferred between participants on a blockchain.[16] Every unit of cryptocurrency is held at an "address." An address is analogous to a safety-deposit box. Just as a safety deposit box stores bars of gold, a cryptocurrency address stores crypto assets

---

[13] Ex. 1, Cole Declaration, ¶¶ 3 – 4 (concluding that Dr. Steinhardt was the victim of a pig-butchering scam and providing sources for comparison to facts of this case).

[14] *Id.*

[15] Ex. 1, Cole Declaration, ¶ 5.

[16] *Id.*

such as Bitcoin.[17] And just as a safety-deposit box can only be opened by a person with its physical key, the assets held at a given cryptocurrency address can only be transferred by a person with its "private key"—a long string of letters and numbers that functions much like a password.[18]

Cryptocurrency addresses differ from safety-deposit boxes, however, in that their transaction histories and balances are *public*.[19] Any person can review the transaction history and asset balances associated with any given address by means of a simple online search.[20] But, because blockchain participants are not required to provide personally identifying information, the identity of the person or persons who control a given address remains obscured.[21] In sum, then, we see that blockchain transactions are both *public* and *pseudonymous*.

To complete our analogy, we can imagine a blockchain as a room filled with safety-deposit boxes. Each box is impenetrable, but also transparent. We can see the assets inside, and each even has a transaction ledger attached. But each box is identified only by a pseudonymous nameplate. We know everything about the boxes—except who controls them.

---

[17] *Id.*

[18] *Id.*

[19] *Id.*

[20] *Id.*

[21] *Id.*

2. Blockchain Tracing

Blockchains' unique characteristics both facilitate investigations and impose inherent limitations. With a few clicks, a crypto-fraud investigator can trace the flow of stolen assets from blockchain address to blockchain address—each transaction representing a "hop," in crypto parlance—and thereby determine where those assets ended up.[22] But, because each address is identified only with a pseudonym, the tracing exercise does not, on its own, reveal *who* is responsible for the scam being investigated.[23]

Despite the pseudonymity of blockchain addresses, there are methods available to discover the identities of the persons controlling a given address. To understand these methods, it is important to understand two concepts: (i) a practice called "address attribution" and (ii) the nature and role of cryptocurrency "exchanges."

Address attribution is the process and practice of gathering and using "off-chain" data to attribute control of a particular blockchain address to a specific person or entity.[24] Investigators frequently take advantage of "attributions" provided by proprietary blockchain-tracing tools.[25] Such tools gather attribution data through open-source intelligence, coordination with

[22] *Id.*

[23] *Id.*

[24] *Id.*

[25] *Id.*

law enforcement, review of judicial filings, "clustering" of addresses whose behaviors reveal common control, and by other means.[26]

One particularly helpful kind of attribution is the association of a particular address with a given cryptocurrency "***exchange***." A cryptocurrency exchange is a platform that allows users to buy, sell, and store cryptocurrencies.[27] Users often choose to use these exchanges for the sake of convenience. Doing so allows them to avoid the difficult technical problems associated with "self-custody" (i.e., the practice of storing cryptocurrencies locally, on devices controlled solely by the user).[28] The result is that, by using a tool like Reactor, investigators can often trace the flow of misappropriated assets to addresses known to be associated with particular exchanges.[29]

The attribution of a particular address in the tracing-path to an exchange provides a unique opportunity to identify the real persons responsible for unlawful activity. Many exchanges require their users to provide know-your-customer and contact information when creating an account, often including the user's real name, date of birth, identity documents, physical address, email address, and phone number.[30] Exchanges also keep records of the balances and transaction histories associated with

---

[26] *Id.*

[27] *Id.*

[28] *Id.*

[29] *Id.*

[30] *Id.*

each customer account.[31] Exchanges routinely provide this biographical and account information to investigators when called to do so.[32]

3. Crypto-Asset Recovery

Useful though it may be, blockchain tracing is not an end in itself. Crypto-fraud victims' goal is to *recover* their stolen assets. But the routes to recovery are limited. As noted above, the nature of blockchain technology is such that only a person with a given address's 'private key' can transfer the assets held at that address.[33] The result is that even where stolen assets can be traced to an address clearly associated with criminality, it is often beyond the power of any court or authority to freeze or disgorge the proceeds of crypto-related crime.[34]

There are, however, exceptions to this rule. Where misappropriated assets can be traced to an *exchange*—as Dr. Steinhardt's investigation has here—the exchange *does* have the power to freeze those assets and ultimately disgorge them as restitution or damages.[35] This is because cryptocurrency exchange accounts do *not* typically operate like the safety-deposit boxes we imagined above. Instead, they operate like checking accounts. When a customer at traditional bank deposits funds in her checking account, the bank

---

[31] *Id.*

[32] *Id.*

[33] *Id.*

[34] *Id.*

[35] *Id.*

does not hold those exact same dollars in segregation until the customer comes back to withdraw them. Instead, the bank intermingles the customer's assets with those it has received from others and simply keeps track of its *indebtedness* to the customer.

Many cryptocurrency exchanges operate in precisely the same way. An exchange customer's account balance does not represent segregated units of cryptocurrency that the exchange holds for that customer—but instead simply tracks the exchange's indebtedness to that customer.[36] This is why exchanges have a special role in crypto-asset recovery. A crypto exchange can "freeze" any account simply by refusing to allow it to engage in further transactions. And it can ultimately transfer assets to victims in its capacity as a crypto-criminal defendant's garnishee.[37]

Two final points about crypto-exchange accounts are important here. First, because exchanges intermingle customer assets, the asset-balance and transaction-history transparency described above are lost where stolen assets are traced to a blockchain address attributed to a crypto-exchange account.[38] Investigators cannot determine the current asset balance or outgoing transaction history of an exchange-associated account using publicly available information.[39] Only the *exchange* has that information, which must

---

[36] *Id.*

[37] *Id.*

[38] *Id.*

[39] *Id.*

be gathered using other means (such as the subpoenas Dr. Steinhardt seeks to issue to the Receiving Exchanges).[40]

Second, because cybercriminals are aware of the vulnerabilities associated with storing assets at cryptocurrency exchanges described above, the asset-recovery opportunities engendered by tracing stolen assets to an exchange are fleeting. Cybercriminals like the Defendants cycle through exchange accounts, using each account only for a short time to marshal, intermingle, and obfuscate the monies they have stolen. They then quickly move to send those assets to non-compliant exchanges or self-custody addresses.[41] When they do so, they are often able to place these assets permanently beyond the reach of any lawful authority.[42] In sum, cryptocurrency exchanges are indeed a chokepoint—but a fleeting one.

D. Blockchain-Tracing Results

Dr. Steinhardt's investigator has traced the assets stolen from Dr. Steinhardt through the blockchain to accounts associated with the following cryptocurrency exchanges (together the "Target Accounts").[43]

---

[40] *Id.*

[41] *Id.* at ¶ 7.

[42] *Id.*

[43] *Id.*

Recipient in Transactions	Associated Entity	Amount Traced (in USD)
0xb4f1c7058ea35690087114f5058ab5b381ce190f8dc072ff6504e722beceec7e 0x6d1305207103561117cb450ef12362e104722ba8186bfd8f4382277713705c0a	Bitget	$100,800.00
0x37e64011b6b6fd8c01db2ee13ce9450562ab4eaf7cee75589ba47712efa4a77c 0x6cb1f65d97af4d548f839a0343ed7863d2d09963f81f646f1da52c2697bbc468 0x3c44e4de6499cb3bbaea23bc9f8f8e821eba2a3e470fb01325fd1b7e9873e0e1 0xf14b3592ed927893f3f4e76a8f2218c6b9dc9369521ca2058845c4ccba0d37fa 0x47af66805c960997a3beb50e4285d782546cfdeb6737f01547e4f0238b29886e	Binance	$170,000.00
0x4cfa7699ade24901b9ae36b6c40fe93b0fb1e8936ac9b676e67ad54df050b92d	Coinbase	$20,000.00

IV. Relief Sought

Dr. Steinhardt seeks (i) a temporary restraining order freezing the Target Accounts and (ii) an order authorizing expedited discovery. The balance of this Motion will articulate the standards applicable to these requests and explain why Dr. Steinhardt has satisfied them.

A. The Court should issue an *ex parte* Temporary Restraining Order freezing the Defendants' accounts at the Target Accounts

Dr. Steinhardt requests that the Court issue an *ex parte* temporary restraining order freezing the assets held by the Target Accounts. The standard for issuance of such an order has both procedural and substantive aspects. This section will first explain why Dr. Steinhardt has satisfied these requirements. It will then detail the Court's authority to issue an asset-freezing order in this case, and why it should indeed do so.

1. Dr. Steinhardt has met the procedural requirements for issuance of an ex parte restraining order.

The Court has the authority to issue an *ex parte* temporary restraining order without notice or a hearing if (i) "specific facts in an affidavit or a verified complaint clearly show that immediate and irreparable injury, loss, or damage will result to the movant before the adverse party can be heard in opposition," and (ii) "the movant's attorney certifies in writing any efforts made to give notice and the reasons why it should not be required."[44] Each of these requirements is met here.

Element 1: Immediate & Irreparable Injury. The Complaint, the Cole Declaration, and the Hoda Declaration show the likelihood of immediate and irreparable injury or loss. These materials first establish that Dr. Steinhardt was victimized by Lena Doe and the operators of the albertAI.click platform

[44] FED R. CIV. P. 65(b)(1)(A)-(B).

in a pig-butchering scam. They do so by providing contextual evidence about the pig-butchering epidemic and comparing that evidence to the Defendants' interactions with Dr. Steinhardt in this case.[45] The tactics on display here are a precise match for those that have been described in news reports, law-enforcement bulletins, and reported cases.[46] Any law-enforcement agent or investigator familiar with this area would conclude that Dr. Steinhardt was the victim of a pig-butchering scam immediately upon reviewing the evidence, just as Dr. Steinhardt's investigator has here.[47]

The risk of immediate and irreparable injury is posed by the fact that cybercriminals like the Defendants can and do move crypto assets from address to address in mere seconds, with the click of a button.[48] And while crypto assets held at exchange-based addresses can be frozen and involuntarily disgorged, most assets held in "self-custody" or at non-compliant exchanges cannot.[49] Thus, the tracing of Dr. Steinhardt's assets to the Target Accounts provides a unique and fleeting opportunity to restrain further movement of those assets while Dr. Steinhardt identifies and serves the Defendants. Courts have repeatedly recognized that these features of

[45] Ex. 1, Cole Declaration, ¶¶ 3 – 5.

[46] *Id.*; Hoda Declaration, ¶ 2.

[47] *Id.*

[48] *Id.* at ¶ 7.

[49] *Id.*

blockchain technology justify the issuance of *ex parte* freezing orders in crypto-fraud cases.[50]

Element 2: Notice. The Court has the authority to enter an *ex parte* order not only where notice to the adverse party is impracticable, but where "notice to the defendant would render fruitless [the] prosecution of the action."[51] Under this logic, courts have found that notice of an asset-freeze motion is not required if the parties to be enjoined "are likely to dissipate assets and destroy business documents," such that the very act of providing

---

[50] *See, e.g.*, *Harris v. Upwintrade*, 1:24-cv-00313-MJT, Dkt. 7 (E.D. Tex.) (Truncale, J.) (Aug. 8, 2024), at p. 9 (granting TRO in functionally identical pig-butchering case and noting "[i]n light of the speed with which cryptocurrency transactions are made, as well as the potential that the Defendants may further move the assets they are alleged to have stolen, the Court finds that the [Plaintiffs'] request to freeze the exchange accounts to which those assets were transferred is justified, as have other courts considering similar circumstances"); *Cohn v. Popescu*, 1:24-cv-00337-MJT, Dkt. 8 (E.D. Tex.) (Truncale, J.) (Aug. 30, 2024) (same); *Ohlin v. Defendant 1*, No. 3:23-cv-8856-TKW-HTC, 2023 WL 3676797, at *3 (N.D. Fla. May 26, 2023) ("Considering the speed with which cryptocurrency transactions are made as well as the anonymous nature of those transactions, it is imperative to freeze the Destination Addresses to maintain the status quo to avoid dissipation of the money illegally taken from Plaintiffs."); *Jacobo v. Doe*, No. 1:22-CV-00672DADBAKBAM, 2022 WL 2052637, at *3 (E.D. Cal. June 7, 2022) ("Because it would be a simple matter for [defendant] to transfer [the] cryptocurrency to unidentified recipients outside the traditional banking system and effectively place the assets at issue in this matter beyond the reach of the court, the court finds that plaintiff is likely to suffer immediate and irreparable harm in the absence of injunctive relief.") (cleaned up); *Astrove v. Doe,* No. 1:22-CV-80614-RAR, 2022 WL 2805315, at *3 (S.D. Fla. Apr. 22, 2022) (same).

[51] *Matter of Vuitton et Fils S.A.*, 606 F.2d 1, 5 (2d Cir. 1979); *see also, e.g.*, *First Tech. Safety Sys., Inc. v. Depinet*, 11 F.3d 641, 650 (6th Cir. 1993) (noting that *ex parte* order is justified under this logic if applicant shows that "the adverse party has a history of disposing of evidence or violating court orders or that persons similar to the adverse party have such a history").

notice would "cause immediate and irreparable, injury, or damages to [the] Court's ability to award effective final relief."[52]

If the Defendants were provided notice of this Motion, it would be "a simple matter" for them to "transfer [the stolen cryptocurrency] to unidentified recipients outside the traditional banking system, including contacts in foreign countries, and effectively put it beyond the reach of this court."[53] Numerous courts, including this Court, have applied just this logic in granting *ex parte* asset-freezing orders in crypto-fraud cases like this one.[54]

---

[52] *Fed. Trade Comm'n v. Dluca*, No. 18-60379-CIV, 2018 WL 1830800, at *2 (S.D. Fla. Feb. 28, 2018), *report and recommendation adopted*, No. 0:18-CV-60379-KMM, 2018 WL 1811904 (S.D. Fla. Mar. 12, 2018).

[53] *Jacobo*, 2022 WL 2052637, at *3 (quoting *Dluca*, 2018 WL 1830800, at *2).

[54] *See, e.g.*, *Harris*, Case No. 1:24-cv-00313-MJT, Dkt. 7, at p. 7 (issuing TRO without notice in pig-butchering case where "the thrust of the [Plaintiffs'] allegations is that the Defendants are professional cybercriminals who have every motivation to place their ill-gotten gains beyond the reach of this Court or any other authority … [and they] have provided sufficient evidence to suggest that the Defendants will in fact further dissipate assets if they were given notice of this motion"); *Gaponyuk v. Alferov*, No. 2:23-cv-01317, 2023 WL 4670043, at *2 (E.D. Cal. July 20, 2023) (issuing *ex parte* asset-freeze TRO in similar crypto-fraud case, and writing that "federal district courts have granted *ex parte* relief in situations like this one, noting the risks that cryptocurrencies may rapidly become lost and untraceable"); *Ohlin*, 2023 WL 3676797, at *2 (notice not required where plaintiff offered declarations showing that the defendants were crypto-criminals, which gave the court "every reason to believe the Defendants would further hide those [stolen] assets if they were given notice"); *Jacobo*, 2022 WL 2052637, at *3 (notice not required because plaintiff made credible allegations that defendants were crypto-criminals, which "pose[d] a heightened risk of asset dissipation").

2. Dr. Steinhardt has met the substantive requirements for issuance of a temporary restraining order.

To obtain a temporary restraining order, the movant must show: (1) a substantial likelihood of success on the merits, (2) a substantial threat of irreparable harm if the injunction does not issue, (3) that the threatened injury outweighs any harm that will result if the injunction is granted, and (4) that the grant of an injunction is in the public interest.[55] Dr. Steinhardt has met each of these requisites for the reasons set out below.

Element 1: The Merits. Dr. Steinhardt alleges that the Defendants are liable for (1) violations of the Racketeering Influenced and Corrupt Organizations Act ("RICO"), (2) conversion, and (3) fraud. She is likely to succeed on the merits of each of these claims.

RICO Claim. To recover on a civil RICO claim, a plaintiff must show (1) a violation of 18 U.S.C. § 1962 (a "RICO violation"), (2) an injury to his business or property, and (3) that such injury was caused by the RICO violation.[56] To prove a RICO violation, a plaintiff must show that the defendant is (1) a person[57] who engaged in (2) a pattern[58] of racketeering

---

[55] *Moore v. Brown*, 868 F.3d 398, 402-03 (5th Cir. 2017).

[56] *Lewis v. Danos*, 83 F.4th 948, 956 (5th Cir. 2023).

[57] A RICO "person" is "any individual or entity capable of holding a legal or beneficial interest in property." 18 U.S.C. § 1961.

[58] A "pattern of racketeering activity requires at least two acts of racketeering activity, one of which occurred after the effective date of this chapter and the last of which occurred within ten years (excluding any period of imprisonment) after the commission of a prior act of racketeering activity." 18 U.S.C. § 1961(5).

activity,[59] (3) connected to the acquisition, establishment, conduct or control of an enterprise.[60]

Dr. Steinhardt's RICO claim is likely to succeed. Her Complaint makes non-conclusory allegations sufficient to establish each element, including by (1) identifying and defining the Defendants' enterprise,[61] (2) explaining their pattern of wire fraud,[62] and (3) recounting the injuries she suffered as a direct result of the Defendants' racketeering scheme.[63] The Complaint and the Cole Declaration show that the Defendants' scheme was the very definition of an enterprise created solely to perpetrate a pattern of wire fraud, and on a global scale.[64] At least one court has issued a default judgment approving a civil RICO claim in a crypto-fraud case functionally identical to this one.[65]

---

[59] "Racketeering activity" includes acts indictable under 18 U.S.C. § 1341 (relating to mail fraud) and § 1343 (relating to wire fraud). 18 U.S.C. § 1961(1)(B).

[60] An enterprise is "a group of persons or entities associating together for the common purpose of engaging in a course of conduct." *Whelan v. Winchester Prod. Co.*, 319 F.3d 225, 229 (5th Cir. 2003) (defining enterprise and recounting elements).

[61] Complaint, ¶¶ 13 – 18.

[62] *Id.*

[63] *Id.*

[64] *Id.*; Cole Declaration, ¶¶ 3 – 5.

[65] Order on Motion for Final Default Judgment, *Sun v. Defendant 1*, No. 1:23-cv-21855 (S.D. Fla. Dec. 8, 2023), pp. 3-4 ("The allegations in Plaintiff's Amended Complaint, admitted by default, establish each element of a RICO § 1962(c) violation. Specifically, Plaintiff alleges that Defendant and her co-conspirators operate a sophisticated global internet cryptocurrency fraud and conversion scheme …").

Conversion Claim. To prevail on a conversion claim, a plaintiff must show (1) she has a right to the property at issue; (2) she has an absolute and unconditional right to the immediate possession of that property; (3) the defendant wrongfully and without authorization assumed control, dominion, or ownership over the property; and (4) she made a demand for the return of the property.[66]

Dr. Steinhardt's conversion claim is likely to succeed. Her Complaint and the Cole Declaration show that the Defendants acted intentionally, that their scheme was wrongful, and that they took control of Dr. Steinhardt's assets and have not returned them.[67] Numerous courts have found that plaintiffs were likely to succeed on conversion claims in in crypto-fraud cases.[68]

Fraud Claim. To prevail on a fraud claim, a claimant must prove: (1) the defendant misrepresented a material fact; (2) the defendant knew the

---

[66] *Apple Imps., Inc. v. Koole*, 945 S.W.2d 895, 899 (Tex. App.–Austin 1997, writ denied).

[67] Complaint, ¶¶ 13 – 17; Ex. 1, Cole Declaration, ¶¶ 3 – 5.

[68] *See, e.g.*, *Bullock v. Doe*, No. 23-CV-3041 CJW-KEM, 2023 WL 9503380, at *5 (N.D. Iowa Nov. 3, 2023) ("Because the claim underlying this request [for an asset-freeze TRO] is mainly conversion—i.e., defendants have plaintiff's property wrongfully—plaintiff's likelihood of success on the merits of this claim suffice for this factor to weigh in favor of plaintiff and the Court need not discuss the further causes of action."); *Yogaratnam v. Dubois*, No. CV 24-393, 2024 WL 758387, at *4 (E.D. La. Feb. 23, 2024) ("It appears from the record that Defendants have no right to claim either possession or ownership of the stolen assets, and Defendants' taking of the funds is clearly inconsistent with Plaintiff's rights of ownership.").

representation was false; (3) the claimant did not know the representation was false; (4) the defendant made the misrepresentation intending that the claimant act on it; and (5) damages resulted from the claimant's reliance.[69]

Dr. Steinhardt's fraud claim is likely to succeed. Her Complaint and the Cole Declaration show that that the Defendants intentionally and falsely represented that Dr. Steinhardt was owed a substantial sum of money for work she performed at what she believed to be a legitimate job, that these representations were material to her, and that she acted on the Defendants' misrepresentations to her detriment.[70]

Element 2: Irreparable Harm. This irreparable-harm requirement is satisfied for the same reasons explained in Section IV(A)(1), above. As noted there, courts have repeatedly found a risk of irreparable harm in crypto-scam cases like this one.[71]

Element 3: Balancing. The threatened injury to Dr. Steinhardt outweighs any damage a freezing order might cause to the Defendants. Dr. Steinhardt has lost a life-changing sum, and the order she seeks is her only hope of preserving some assets for recovery. And while an asset freeze might cause temporary inconvenience to the Defendants, any restraint

---

[69] *JPMorgan Chase Bank, N.A. v. Orca Assets G.P., L.L.C.*, 546 S.W.3d 648, 653 (Tex. 2018).

[70] Complaint, ¶¶ 15 – 27; Ex. 1, Cole Declaration, ¶¶ 3 – 5.

[71] *See* n.55, *supra* (collecting cases).

implemented can be undone should future developments require.[72] In addition, should the Court grant Dr. Steinhardt's requests for expedited discovery and her forthcoming request for substituted service, the Defendants are highly likely to receive actual notice of this proceeding in the near term. They will then have every opportunity to appear and seek dissolution of any freeze implemented.

Element 4: Public Interest. A freezing order will serve the public interest because it will "dissuade would-be fraudsters from stealing, laundering illegal proceeds, and preying on Americans" like Dr. Steinhardt.[73] It will also "prevent the Defendants from profiting from their scheme, ensuring they lack resources and incentives to perpetrate similar schemes in the future,"[74] and "provide[] assurance to the public that courts will take action to promote … recovery of stolen assets when they can be readily located and traced to specific locations."[75]

---

[72] *See, e.g.*, *Licht*, 2023 WL 4504585, *3 (balancing factor weighed in plaintiff's favor because alleged crypto-thieves faced only "inconvenience" of asset-freeze, which could be undone); *Gaponyuk*, 2023 WL 4670043, at *3 (same, finding "a short-term freeze is unlikely to present any great harms"); *Jacobo*, 2022 WL 2052637, at *6 (same, finding "[a] delay in defendant's ability to transfer the [allegedly stolen] assets only minimally prejudices defendant, whereas withholding injunctive relief would severely prejudice plaintiff by providing defendant time to transfer the allegedly purloined assets into other accounts beyond the reach of this court").

[73] *Licht*, 2023 WL 4504584, at *3.

[74] *Id.*

[75] *Jacobo*, 2022 WL 2052637, at *6 (quoting *Heissenberg*, 2021 WL 8154531, at *2); *see also, e.g.*, *Gaponyuk*, 2023 WL 4670043, at *3 (finding

3. The Court has the authority to issue the asset-freezing injunction Dr. Steinhardt seeks.

Typically, a court may issue an order freezing a defendant's assets only after a plaintiff's claims have been brought to judgment.[76] This rule does not apply, however, where the plaintiff seeks equitable relief and a constructive trust over traceable stolen assets.[77] Dr. Steinhardt seeks just such relief here.[78] For that reason, the Court has the authority to issue the asset-freezing injunction Dr. Steinhardt seeks.

4. The Court should not require a bond.

Rule 65(c) provides that a court issuing a preliminary injunction or TRO should do so "only if the movant give security in an amount that the court considers proper to pay the costs and damages sustained by any party found to have been wrongfully enjoined or restrained."[79] Yet, "[c]ourts retain extensive discretion to set the amount of a bond required as a condition for issuing a preliminary injunction and may, in fact, elect to require no bond at

---

that asset freeze would "serve the public's interest in stopping, investigating, and remedying frauds").

[76] *Grupo Mexicano de Desarrollo S.A. v. Alliance Bond Fund, Inc.*, 527 U.S. 308, 322 (1999).

[77] *See, e.g.*, *Yogaratnam v. Dubois*, No. CV 24-393, 2024 WL 758387, at *3 (E.D. La. Feb. 23, 2024) (issuing asset-freeze TRO in crypto-fraud case, noting that "numerous district courts … have issued a TRO in this exact circumstance to freeze a cryptocurrency asset," and collecting cases); *Jacobo*, 2022 WL 2052637, at *3 (issuing asset-freezing TRO where plaintiff sought constructive trust over allegedly stolen assets); *Gaponyuk*, 2023 WL 4670043, at *2 (same).

[78] Complaint, ¶ 33.

[79] FED. R. CIV. P. 65(c).

all."[80] The Defendants will not suffer any damages as a result of the requested asset freeze, which—as explained above—can be undone at any time if the Defendants choose to appear and challenge the injunction. Dr. Steinhardt thus requests that the Court decline to impose a bond.

B. The Court should authorize Dr. Steinhardt to issue subpoenas seeking information about information about the Defendants and their activities.

Typically, parties may not seek "discovery from any source before the conference required by Rule 26(f)."[81] But expedited discovery before a Rule 26(f) conference is permitted where "authorized … by court order."[82] Courts in this circuit apply a "good cause" standard to determine whether such an order should issue.[83] Good cause may be found where "the need for expedited discovery in consideration of the administration of justice, outweighs the prejudice to the responding party."[84]

Many courts, including this Court, have authorized expedited discovery from cryptocurrency exchanges in cryptocurrency-related fraud cases like this one.[85] Indeed, courts have affirmatively held that any privacy

---

[80] *Astrove*, 2022 WL 2805345, at *5 (declining to require bond in crypto-theft case); *Jacobo*, 2022 WL 2052637, at *6 (same).

[81] FED R. CIV. P. 26(d)(1).

[82] *Id.*

[83] *St. Louis Grp., Inc. v. Metals & Additives Corp.*, 275 F.R.D. 236, 239 (S.D. Tex. 2011) (applying good cause standard).

[84] *Id.* at 239.

[85] *See, e.g.*, *Strivelli v. Doe*, No. 22-cv-22060 2022 WL 1082638, at *2 (D.N.J. Apr. 11, 2022) (authorizing expedited discovery from cryptocurrency

interests that alleged cybercriminals have concerning the discovery of information about their identities and activities is outweighed by the need to adjudicate victims' claims against them.[86]

1. Proposed Discovery

Dr. Steinhardt's proposed discovery arises from her pre-suit investigation. This investigation revealed a series of third parties likely to be in possession of information about the Defendants. Each of those third parties and their connection to this case is set out below. These connections are attested to in the attached declaration of Dr. Steinhardt's investigator.[87]

Subpoena Target	*Connection to Case*
Coinbase	Plaintiff's assets were traced to a deposit address or addresses at this exchange.
Bitget	Plaintiff's assets were traced to a deposit address or addresses at this exchange.

exchanges in crypto case and noting "the Court's review of cryptocurrency theft cases reveals that courts often grant motions for expedited discovery to ascertain the identity of John Doe defendants"); *Licht*, 2023 WL 4504585, at *4 (issuing broad authorization for expedited discovery in functionally identical crypto-fraud case and requiring that "any party served with a request for production shall produce all requested items within 72 hours of the request").

[86] *Gaponyuk*, 2023 WL 4670043, at *4 (finding alleged cybercriminals' privacy interests were "outweighed by the need to adjudicate the [victim's] claims," and holding that "privacy concerns shall not be a just cause for [a] subpoenaed non-party to withhold [] requested documents and information").

[87] Ex. 1, Cole Declaration, ¶¶ 9 – 10.

Binance	Plaintiff's assets were traced to a deposit address or addresses at this exchange.
NameSilo	NameSilo is the domain registrar for one of the alleged scammers' web domains.
Tucows	Tucows is the domain registrar for one of the alleged scammers' web domains.
Cloudflare	All of the alleged scammers' web domains used Cloudflare's content-delivery services.
WhatsApp	The alleged scammers used WhatsApp to communicate with Dr. Steinhardt.

2. Information Sought

Dr. Steinhardt seeks the Court's authorization to issue subpoenas to each of the above-listed entities seeking the following information. Dr. Steinhardt seeks to discover all biographical and contact information associated with the Defendants' accounts. She also seeks to discover IP-address and location logs showing the devices and locations from which the Defendants accessed these accounts.

Dr. Steinhardt also seeks to discover any payments information in the subpoena targets' possession, including the Defendants' transaction histories and information about the credit or debit cards the Defendants used to pay for the subpoena targets' services. As to the Defendants' payment methods,

Dr. Steinhardt seeks only information sufficient to identify the Defendants' payments provider and the Defendants' account with that provider.

Courts, including this Court, have authorized similar discovery where the plaintiff adduced evidence that the persons about whom the information was sought were cybercriminals and the plaintiff also sought a temporary restraining order freezing the assets held in those accounts.[88]

V. Conclusion

For the reasons set out above, Dr. Steinhardt has met the standards for issuance of a temporary restraining order and an order authorizing expedited discovery in this matter. She requests that the Court issue this relief in the form of the proposed order submitted with this Motion.

[88] *See, e.g.*, *Harris v. Upwintrade*, 1:24-cv-00313-MJT, Dkt. 7 (E.D. Tex.) (Truncale, J.) (Aug. 8, 2024) (granting expedited discovery in functionally identical pig-butchering case); *Cohn v. Popescu*, 1:24-cv-00337-MJT, Dkt. 8 (E.D. Tex.) (Truncale, J.) (Aug. 30, 2024) (same); *Strivelli*, 2022 WL 1082638, at *2 (granting broad expedited discovery in functionally identical crypto-fraud case); *see also Licht*, 2023 WL 4504585, at *4 (same).

Dated: June 16, 2025

Respectfully submitted,

THE HODA LAW FIRM, PLLC

Marshal J. Hoda, Esq.
Tx. Bar No. 2411009
Alexander J. Crous
Tx. Bar No. 24136488
12333 Sowden Road, Suite B
PMB 51811
Houston, TX 77080
o. (832) 848-0036
marshal@thehodalawfirm.com

Attorney for Plaintiff